Stock Price Reaction To Data Breaches

Mark S. Johnson, Min Jung Kang, and Tolani Lawson

Abstract

Data Breaches occur in many forms that include bad security practices, hacking, insider attacks, stolen or lost equipment and computer or data theft. Data breaches happen to organizations of all types. In this paper, we present an analysis of the stock market's assessment of the cost of data breaches through the examination of 467 heterogeneous data breach events that occurred at 261 publicly traded companies between year 2005 and 2014. Our event study findings indicate that publicly traded firms in the U.S. lost, on average, .37% of their equity value when a data breach occurs. Particularly, we find that breaches resulting from payment card fraud contributed more to negative announcement returns than the other breach types. Such negative announcement effects are most heavily felt when firms with card breaches are larger than the average, resulting in a 3% decline in firm equity value. Contrary to previous studies, we find that repeated breaches do not impact firm stock value differently than first-time-breaches. However, we find that there is a high correlation between firm size and the existence of multiple, repeat, data breaches. This implies that large firms hit by a data breach are more likely to experience subsequent breaches than small firms.

I. Introduction and Study Context

As computer and online activity continues to increase, it is imperative that managers understand more fully what financial consequences occur with different types of data breaches. Data breaches include computer hacking, lost or stolen computer equipment, and employee data theft. The costs to companies of data breaches include both direct costs like reimbursement of customer losses and indirect costs like loss of consumer/investor confidence. In addition, potential litigation may be incurred, which will additionally incur direct and indirect costs associated with the litigation. The Ponemon Institute reports that U.S. companies incurred $5.4 million in direct costs, on average, for each data breach that occurred. The urgency for U.S. firm mangers to understand the costs of data breaches is borne out by the fact that direct costs per breach incurred by U.S. firms is higher than the direct costs incurred by companies domiciled in any other country in the world (Ponemon 2015, Spiderlab 2015).

This paper analyses the consequences associated with data breaches in a large sample of heterogeneous publicly traded firms. Particularly, the paper examines stock price announcement effects associated with a data breach to determine the direct and indirect costs stemming from the loss of investor confidence. Examining the stock price behaviour is important because stock price reflects current, expected future costs and risk associated with a data breach from the investor's point of view. It is also important to the affected firm's management teams because stock price reflects firm value, which indicates overall strength and health of a company, the factors that is critical in determining firm's future cost of capital, credit ratings, employees' and manager's compensation, management team's firing decision and etc. Most importantly, publicly traded companies' management teams are hired

Mark S. Johnson works at the Department of Finance, The Eli Broad School of Business, Michigan State University, 324 Eppley, East Lansing, MI 48824-1121.; Min Jung Kang is an assistant professor at the Department of Finance, School of Management, University of Michigan-Flint, 2138 Riverfront center, 303 Kearsley Street, Flint, MI 48502-1950.; Tolani Lawson is a senior financial analyst at the Westrock Company, 5800 W. Grand River Avenue, Lansing, MI 48906.

to represent the owners, whom are the shareholders. Hence, increase (decrease) in share price often indicates an owner's value increasing (decreasing) behaviour by the management.

The paper has three goals. Our primary goal is to determine the average announcement effect on the stock market of all types of data breaches on a wide variety of publicly traded firms. Our secondary goal is to determine what, if any, types of data breaches are worse for the average firms in the market. Our tertiary goal is to determine the influence of repeat breaches, firm size and size of data breach on firm value. This should help managers determine the degree of their risk exposure and the level of effort that should be expended on cyber security in their firms.

The motivation for this paper is similar to previous papers in that we wish to determine the impact of data breaches on firm value. However, our research extends the prior literature on data breaches with a larger and longer-period data set. With its large heterogynous sample of data breaches, we provide results that are more representative of all data breaches than previous studies. Additionally, with a larger sample size, it is possible to have greater confidence in any second order effects that are found to differentiate firms within the sample. We also include different types of data breaches, which makes the analysis more interesting by examining the impact on stock values depending on the type of breaches and whether the corresponding announcement effects are different from one another. In addition, our study controls for other confounding effects to solely recognize the data breach event effect on the stock price, which has been rarely done in prior data breach event study papers.

II. Literature review

Previous literature looking at the impact of data breaches on firm value has provided mixed results. Some of the studies have found significant negative impacts and some have only found little to no support for the idea that data breaches impact firm value. For a summary of these results, see Table I below. Previous studies have mostly focused on breaches that were reported in major news publications such as the Wall Street Journal and USA Today. Some studies found overall negative effects (Garg et al., 2003; Cavusoglu et al., 2004; Gatzlaff et al., 2010; Acquisti et al., 2006) while others find no significance associated with data breach announcements (Campbell et al., 2003; Hovav et al., 2003; Kannan et al., 2007). However, these studies have used relatively a small number of data breaches to draw conclusions, as can be seen in Table I in sample size column.

Table I. Summary of Previous Data Breach Event Studies

Paper	PublicationDate	Sample Size	Data Years	Window	CAAR Entire Sample
Acquisti et al.	2006	79	2000-2006	2 day	-.58%
Campbell et al.	2003	43	1995-2000	3 day	insignificant
Cavusogluet al.	2004	66	1996-2001	2 day	-2.1%
Garg et al.	2003	22	1996-2002	3 day	-5.3%
Gatzlaff et al.	2010	77	2004-2006	2 day	-.46%
Hovav et al.	2003	23	1998-2002	3 day	Insignificant
Kannan et al.	2004	102	1998-2002	4 day	Insignificant
This paper		467	2005-2014	3 day	-.37%

III. Hypothesis development

The first goal of this paper is to discover the extent to which data breaches impact the value of firms. The previous literature indicates that the overall impact on firms experiencing data breaches is either negative or zero. Hence, our first hypothesis, stated in the null, becomes:

H1: The average abnormal return associated with the 3-day event breach window is zero on average for the firms in the sample.

We also develop three categories of hypotheses about how the impact of data breaches varies across firms based on firm type, breach type, and the possible unique characteristics of the data breach. For firm type, firms were first split into financial and insurance services, retail/merchant and others. These groupings are provided by Privacy Rights Clearing House, 2014, which provided the data breach dates and information. Other potential grouping of firms was considered but the grouping provided by privacy rights clearing house clearly separated firms that are financial intermediaries from those which primarily provide goods and service. To examine how different breach types impact firm's variables used for data breaches are split into 7 breach types as classified by the Privacy Rights Clearing House, 2014. Finally, breach/firm characteristics are potentially thought to influence the size of any data breach impact on firm wealth. These characteristics are whether the breach has been experienced repeatedly by the firm (REPEAT), whether a firm has a market capital above 10billion (LARGECAP), and how large the breach size is (BREACH_SIZE). Table II below shows the definition of independent variables used in the three groups of hypotheses.

Table II. Definition of Independent Variables

Variables	Expected Result	Definition
Firm Type		
BSF	Negative	Businesses - Financial and Insurance Services - US publicly listed firms in the financial and insurance services
BSR	Negative	Businesses - Retail/Merchant - US publicly listed firms in the retail industry
OTH	Negative	Businesses - Includes a wide variety of firms that cannot be classified as either retail or financial.
Data Breach Type		
CARD	Negative	Payment Card Fraud- Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
DISC	Negative	Unintended disclosure - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
HACK	Negative	Hacking or malware - Electronic entry by an outside party, malware and spyware.
INSD	Negative	Insider - Someone with legitimate access intentionally breaches information - such as an employee or contractor.

PHYS	Negative	Physical loss - Lost, discarded or stolen non-electronic records, such as paper documents
PORT	Negative	Portable device - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc
STAT	Negative	Stationary device - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
Firm and breach Characteristics		
REPEAT	Neutral	A proxy for breaches that represent a repeated occurrence for the individual firm.
LARGECAP	Negative	A proxy for the size of the firm based on its market capital. This represents large companies with a market capital above $10 billion
BREACH_SIZE	Negative	A proxy for the size of the breach based on the number of records affected. This represents breaches affecting over a hundred thousand records

Stated as the null hypothesis:

H2: Firm type do not matter. That is, financial and insurance firms are not significantly different from other firms in the sample. And retail and merchant firms are not significantly different from other firms in the sample.

H3: Breach characteristics don't matter. That is CARD, DISC, HACK, INSD, PHYS, PORT, STAT breaches are no different from other breaches in the sample.

H4: Firm and breach characteristics don't matter. That is, REPEAT breaches are no worse than original breaches, LARGE CAP firms are no more heavily impacted than small cap firms and the amount of information breached, BREACH SIZE, doesn't matter.

IV. Event Study Research design

The sample used for this study consists of instances of data breaches in publicly traded entities over 10 years. This sample was derived by collecting a list of all data breach announcements from the privacy rights clearing house. The privacy rights clearing house is non-profit organization that "educates and empowers" individuals to protect their privacy. This organization acquires observations from sources such as the Open Security Foundation, DataBreaches.net, PHI Privacy, and NAID. By closely monitoring several media outlets, government websites, and blog posts, these sources are combined to provide the most comprehensive dataset for privacy breach events. The reported breaches in database from the privacy rights clearing house consists of breach reports that have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. We chose this medium for selecting our sample because we wanted to develop a sample that was representative of the population of all information security breaches. This research relies on the most comprehensive data set available that extends beyond the traditional use of newspapers as the sole source of breach announcement dates and related data.

Our search for information security breaches covers the period January 2005 through December 2014. The raw dataset obtained from Privacy Rights Clearing House, 2014, contained 1,715 data breach events in sectors including business, educational institutions, government/military, healthcare/medical providers, and non-profit organizations. This list was then sorted for publicly traded companies in the United States, and narrowed our initial selection down to 497 data breach events. Additional sample selection criteria are the availability of sufficient returns history (i.e., a minimum public trading history) on the Center for Research in Security Prices (CRSP) database for the estimation period necessary for our event study, continuity in the corporate entity's identity over the period, and elimination of multiple events where estimation periods overlap earlier events for the same firm. When there was an overlap in the estimation period with a prior event for the same firm, we used the earlier event reporting date and dropped an observation. Using these criteria eliminated thirty breaches, leaving us with 467 data breach events in 261 unique publicly listed US firms. Table III Panel A provides a breakdown of the sample of breaches by breach type and firm type. Clearly all types of firms have experienced a wide variety of data breaches with no obvious grouping within a given sector. Table III Panel B provides a breakdown of the sample by year. Over the 10-year period there appears to be significant variability in the number of breaches reported. However, there does not appear to be a clear upward or downward trending in the number of breaches over time.

Table III

Panel A: Data Breaches by Firm Type and Breach Type

	CARD	DISC	HACK	INSD	PHYS	PORT	STAT	UNKN	Total
BSF	13	32	29	29	8	43	6	11	171
BSR	8	22	38	39	10	33	5	5	132
Others		24	35	12	2	52	6	5	136
Total	21	78	102	80	20	128	17	21	467

Panel B: Data Breaches by Year

	'05	'06	'07	'08	'09	'10	'11	'12	'13	'14	Total
No. of Breaches	23	64	63	28	75	10	57	61	66	20	467

V. Test of Market Reaction

The first hypothesis is tested by examining the overall industry market reaction to the reporting date of each data breach event. The market reaction was determined by measuring daily abnormal returns (ARs), i.e., the difference between actual and expected returns. To control for the effects of market-wide fluctuations, the market model is used to measure expected returns:

$$R_{it} = \alpha_i + \beta_i R_{mt} + e_{it}$$

where R_{it} is the return for the ith data breach event on day t, α_i is the intercept for the ith data breach event, β_i is the slope coefficient for the ith data breach event, R_{mt} is the return on an equal-weighted market portfolio on day t, e_{it} is the error term with mean zero.

Following the findings of Brown and Warner (1980, pp. 242–243); Brown and Warner (1985, p. 12); and Binder and Summer (1985, p. 173), an equal-weighted market index is used as a proxy for the market rate of return. The parameters α_i and β_i were estimated for the event by using 255 trading days of daily return data ending 30 days prior to the breach

being reported. Generally speaking, in event studies, we want the parameters of the model to be estimated over a short time period before the event occurs. This involves a trade-off. The closer the estimation period is to the event period; the less likely it is that sample firm betas have changed due to changes in leverage, management strategy, and firm investments, etc. But, estimation data from a period too close to the event period may be contaminated by abnormal returns that were caused during previous regulatory announcements or proceedings. We choose to estimate the parameters of the model using 255 days of data ending 30 days prior to the breach being reported. We did this to, as much as possible, avoid confounding information about the data breach event that could potentially bias the estimates. Once the parameters α_i and β_i have been estimated for each firm, the daily prediction errors (abnormal returns) for firm *i* was calculated as follows:

$$AR_{it} = R_{it} - [\alpha_i + \beta_i R_{mt}]$$

where AR_{it} is the abnormal return for firm *i* on day *t*.

We examine abnormal returns for the three-day window that includes the event day and the two trading days immediately before and after the event. Inclusion of the trading days prior to the event controls for information leakage that may occur if some market participants are privy to the information prior to public announcement of policy actions. Inclusion of the trading days after the event accounts for late arrival of information to the market or adjustment to information that requires time for market participants to interpret. A window that is too large will include extraneous information. Conversely, a window that is too small will not fully capture the effects of information leakage or slow market adjustment. We choose a window of 3-days. Thus, our results are reasonably conservative and should cover a significant amount of the impact of the data breach. While there is nothing unique about the choice of this 3-day window it seems to fall within the realm of that used by previous researchers see Table I. The three day cumulative abnormal returns for each firm were computed as below:

$$CAR_i = \sum_{t=-1}^{+1} AR_{it}$$

where CAR_i is the cumulative abnormal return for data breach event *i,* AR_{it} is the abnormal return for data breach event *i* on day *t,* and *t*=0 is the day the data breach is reported to the government.

To determine the average overall impact of the events on the industry, we calculate the three-day cumulative average abnormal return by summing across the *n* firms in the sample and dividing by the number of firms in the sample as below:

$$CAAR = \sum_{i=1}^{n} CAR_i/n$$

where *CAAR* is the cumulative average abnormal return across all events in the sample, and CAR_i is the 3-day cumulative return for data breach event *i* around the event. CAAR is the 3-day cumulative average abnormal returns for the sample of *n* data breach events. To examine whether each informational event had a significant average return effect on the industry, a test of the null hypothesis that the three-day cumulative average abnormal return across firms equals zero is performed using a Z statistic.

VI. Cross-sectional analysis

Cross-sectional analysis is employed to test the three groups of hypotheses that differences in abnormal returns across firms are explained by the firm type, breach type, and the characteristics of the data breach. Specifically, multiple regression analysis is used to examine the relationship between the market reactions to each data breach event based on the variables in these three separate categories.

The first category is firm type. Two variables are used to represent each firm type and a dummy variable that equals one for the corresponding variable and zero if it is not. We estimate the following multiple regression model for the total sample:

$$CAR_i = \gamma_0 + \gamma_1 BSR_i + \gamma_2 BSF_i$$

where CAR_i is the 3 day cumulative return for firm *I,* BSR_i is a dummy variable that equals one if the firm involved in the breach is a retail firm, and BSF_i is a dummy variable that equals one if the firm involved in the breach is a financial and insurance services firm. γ_0, γ_1, γ_2,, are the estimated intercept and two slope coefficients. γ_1 , γ_2,, provides a potential estimate of the additional impact that may exist for re the estimated intercept and two slope coefficients, respectively.

The second category is the breach type. Seven variables are used to represent each breach type and a dummy variable that equals one for the corresponding variable and zero if it is not. We estimate the following multiple regression model for all available observations in the sample:

$$CAR_i = \gamma_0 + \gamma_1 CARD_i + \gamma_2 DISC_i + \gamma_3 HACK_i + \gamma_4 INSD_i + \gamma_5 PHYS_i + \gamma_6 PORT_i + \gamma_7 STAT_i$$

where CAR_i is the 3 day cumulative return for firm *I,* $CARD_i$ is a dummy variable that equals one if the type of breach is a payment card fraud, $DISC_i$ is a dummy variable that equals one if the type of breach is an unintended disclosure, $HACK_i$ is a dummy variable that equals one if the type of breach is a hack breach, $INSD_i$ is a dummy variable that equals one if the type of breach is an insider breach, $PHYS_i$ is a dummy variable that equals one if the type of breach is a physical loss, $PORT_i$ is a dummy variable that equals one if the type of breach is a portable device breach, and $STAT_i$ is a dummy variable that equals one if the type of breach is a stationery device breach. γ_0, γ_1, γ_2, γ_3, γ_4, γ_5, γ_6, γ_7, are the estimated intercept and seven slope coefficients, respectively. Our second hypothesis predicts that the estimated coefficient on *CARD*, γ_1, will be negative and less than the other coefficient.

The third category is the characteristics of the data breaches. Four variables are used to represent each characteristic and a dummy variable that equals one for the corresponding variable and zero if it is not. We estimate the following multiple regression model for all available observations in the sample:

$$CAR_i = \gamma_0 + \gamma_1 REPEAT_i + \gamma_2 LARGE\_CAP_i + \gamma_3 BREACH\_SIZE_i$$

where CAR_i is the 3 day cumulative return for firm *i,* $REPEAT_i$ is a dummy variable that equals one if the a repeated occurrence for the firm, $LARGE\_CAP_i$ is a dummy variable that equals one if the involved firm's market capital is above $10 billion, and $BREACH\_SIZE_i$ is a dummy variable that equals one if the number of records involved is over a hundred thousand records. γ_0, γ_1, γ_2, γ_3, are the estimated intercept and four slope coefficients, respectively. Our hypothesis predicts that the estimated coefficient on REPEAT, γ_1, LARGE_CAP, γ_2, and BREACH_SIZE, γ_3, will be non-zero. The results of the cross-sectional analysis are discussed in Section VI.

VII. Results

Table IV presents our test of hypotheses H1, which tests whether there is a significant negative effect on stock returns from data breaches. H1 was first tested by examining the overall industry market reaction to the reporting date of each data breach event with CAAR, the Cumulative Average Abnormal Return, which is an average of individual firm CARs. The CAAR is -0.37% for the entire sample of publicly traded firms as shown in Panel A of Table IV. The p-value for the appropriate test statistic, Patell Z, is .0019. Therefore, we conclude that the effect, while small, is significant and negative for any reasonable decision criteria. Also, as can be seen from Panel B of Table IV, there is no difference in market reaction to data breaches.

Table IV. Cumulative Average Abnormal Return (CAAR)

Panel A: over a 3-day event window

Event Tested	*n* (Number of Events)	3-Day CAAR[1]	Pos:neg[2]	Generalized Z-Statistic[3] (p-Value)	Patell Z-Statistic[4] (p-Value)
Data Breaches	467	-0.37%	203:264	-2.053 (0.0200)	-2.893 (0.0019)

1. CAAR is the average abnormal return for the of *an* event breaches in our sample over the three day event window, day before, day of and day after each data breach event. Abnormal returns are calculated using an equal weighted market index. 2. The number of firms with positive CAR versus a negative CAR in the sample. 3. Generalized Z-Statistic, one of the most commonly used one-tail test of significance different from zero. 4. Patel Z-Statistic, one of the most commonly used, in event studies, one-tail test of significance different from zero.

Panel B: change in market reaction: 2005-2009 vs 2010-2014

t-Test: Two-Sample Assuming Unequal Variances		
	CAAR	*CAAR*
	2005 to 2009	*2010 to 2014*
Mean	-0.004370222	-0.00317
Variance	0.001044889	0.00102
Observations	197	270
Hypothesized Mean Difference	0	
df	420	
P(T<=t) one-tail	0.3457172	
t Critical one-tail	1.648489713	
P(T<=t) two-tail	0.6914344	
t Critical two-tail	1.965628284	

In Figure I, we visually present the cumulative average abnormal return for the entire sample from 7 days before the announcement to day x, represented in the horizontal axis. We do this to help us look for the possibility of inefficiency with respect to the market incorporating the breach news. That is, the CAAR drops off quickly around the event and does not rebound. Hence, information leakage, over-reaction and under-reaction do not appear to be present in the study.

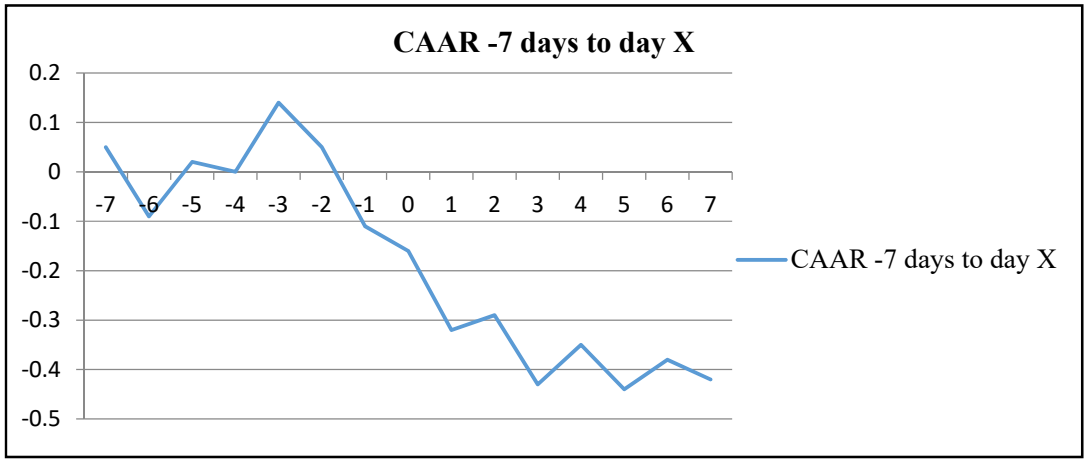

Figure I. CAARs starting 7 days before- and ending 7 days after- the event day

Table V Panel A presents the mean, standard deviation, maximum and minimum values for the dependent variable CAAR grouped by firm type, data breach type and firm characteristics. Visually there appear to be differences between the different groups but it is not obvious whether or not these differences are significantly different. It is worth noting that all but one of the subgroups experienced a negative CAAR associated with data breaches and that none of the subgroups reveal a zero effect. In fact, INSD, insider revealing information, may have very little effect on firms. We also not that standard deviation with between groups varies from 2.4% to 6.1%. This may indicate that the spread of outcomes is different between groups in the sample. Panel B of Table V presents correlation among the independent variables, except the dummy variables, used in the cross sectional regression analysis. It may be worth noting that the correlation between all of the independent variables is relatively low with the highest correlation existing between Large Cap and Repeat. This seems to say that Large Cap firms may be more likely to have multiple breaches after they have experienced their first breach.

Table V. Descriptive Statistics

Panel A: Descriptive Statistics for CAAR by firm type and breach type.

	Mean Percent Cumulative Abnormal Return	Minimum Percent Cumulative Abnormal Return	Maximum Percent Cumulative Abnormal Return	Standard Deviation Cumulative Abnormal Return
Firm Type				
BSF	-0.256	-14.292	8.097	3.171
BSR	-0.675	-22.813	13.893	3.689
OTH	-0.146	-9.892	9.036	2.574
Data Breach Type				
CARD	-1.673	-21.304	4.8722	6.090
DISC	-0.400	-12.214	6.893	2.748
HACK	-0.587	-22.813	13.894	3.910
INSD	0.0566	-8.129	7.578	2.448
PHYS	-0.714	-6.15	7.703	2.668

PORT	-0.269	-5.985	9.036	2.446
STAT	-0.629	-5.556	6.344	2.463
Firm Characteristics				
REPEAT	-0.310	-8.129	13.894	2.614
LARGE_CAP	-0.405	-22.813	8.097	2.777
BREACH_SIZE	-1.860	-14.292	3.968	4.868

Panel B: Correlation coefficients between breach type and firm characteristics.

	CARD	*DISC*	*HACK*	*INSD*	*PHYS*	*PORT*	*STAT*	*REPEAT*	*LARGE CAP*	*BREACH SIZE*
REPEAT	0.078	0.065	-0.042	0.203	-0.018	-0.179	-0.104	1		
LARGE_ CAP	0.016	-0.014	0.017	0.067	-0.128	-0.002	-0.063	0.321	1	
BREACH _SIZE	0.060	-0.005	0.049	-0.065	-0.044	0.044	-0.040	-0.052	-0.092	1

Table VI provides the results of four different cross-sectional regressions. The first regression, in Panel A, examines firm type, retail and financial. There is no support for the idea that either type of firm is likely to have greater than average value effects from a data breach. The regression in Panel B indicates that data breach incidents that occur as a result of payment card fraud (CARD) more negatively affect the firms in our sample than any other type of data breach. This result is significant at a 3.3% level and supports hypothesis. This implies that the average firm experiencing a CARD incident suffers a -1.67% change in firm value (sum of intercept and slope).

The regression in Panel C indicates data breach incidents that affect over a hundred thousand records (BREACH_SIZE) have a negative effect on the returns of the afflicted firms such that the average firm with large breach size experienced a CAAR of -1.79%. This result is significant at a 3.6% level. The regression also indicates that if a firm experiences multiple data breaches (REPEAT), the subsequent breaches are not more or less costly than the initial breach. Finally, in Panel D the regression is rerun with the only independent variables from Panels A, B and C that were significantly different than zero. We find that both slope coefficients remain significant at the 10% level and are qualitatively of similar size and magnitude as those in the previous regressions. The regression indicates that card data breaches with large loss of data might be expected to exhibit a 3% negative CAAR. This result helps to explain how previous studies have had such a wide range of CAAR estimates. Clearly, firms with the attributes mentioned above experience very large, negative, CAARs while most firms experience very small negative CAARs associated with data breaches.

Table VI. Multiple regression of 3-day CAR_i[1,2].

Panel A			
	Coefficient	t-Statistic[3]	P-value
Intercept	-0.00146	-0.53181	0.59511
BSR	-0.00529	-1.41514	0.1577
BSF	-0.00110	-0.29908	0.76501
R^2= 0.00500			

Adjusted R^2= 0.00071			

Panel B			
Intercept	0.00445	0.63625	0.52493
CARD	-0.02118	-2.14088	0.03281
DISC	-0.00845	-1.07260	0.28402
HACK	-0.01032	-1.34350	0.17977
INSD	-0.00389	-0.49429	0.62134
PHYS	-0.01159	-1.15739	0.24771
PORT	-0.00714	-0.94594	0.34468
STAT	-0.01074	-1.02682	0.30505
R^2= 0.01541			
Adjusted R^2= 0.00040			

Panel C			
Intercept	-0.00211	-0.76692	0.44352
REPEAT	0.00138	0.43673	0.66251
LARGE_CAP	-0.00225	-0.66706	0.50506
BREACH_SIZE	-0.01586	-2.10562	0.035775
R^2= 0.01027			
Adjusted R^2= 0.00386			

Panel D	Coefficient	t-Statistic[3]	P-value
Intercept	-0.00250	-1.62830	0.10414
CARD	-0.01283	-1.79858	0.07274
BREACH_SIZE	-0.01475	-1.97121	0.04930
R Square= 0.01606			
Adjusted R^2= 0.01182			

1. CAR_i is the three day cumulative abnormal return for data breach event *i* around the date of reporting the data breach to the government.
2. The regression was also performed with CAR regressed on all 14 independent variables in one regression equation. The results were qualitatively very similar to the individual regressions slope coefficients and p-values.
3. This is a two-tailed t-test of the hypothesis that the slope coefficient is not equal to zero. P-values give the level of confidence for the t-test.

VIII. Summary and conclusions

We examined the market reaction of 467 heterogynous data breaches and found that the average decline in firm value from a data breach was .37%. Unlike some previous studies, we find that firm type is not a major determinant in the effect of data breaches on stock price. Our cross-sectional regression results show that breaches resulting from payment card fraud contributed more to negative returns than the other breach types and that the most heavily hit firms were those where the card breaches were larger than average. In fact, when Card breaches were large the average firm experienced a 3% decline in value. Contrary to previous studies we find that repeat, versus first time breaches, do not impact firms differently than first time breaches. However, we find that there is a high correlation between firm size and the existence of multiple, repeat, data breaches. That is, large firms hit by a data breach may be more likely to experience subsequent breaches than small firms.

The implications of our results for managers are many. First, we find that managers should be alarmed about data breaches. Under the wrong circumstances the impact of a data breach can be quite large. Managers need to be aware that the majority of data breaches do not have extremely large impacts on firm value (-.37% on average). Thus, managers can take most data breaches in stride and deal with them when they arise. However, Managers should be aware that the real value changer for the firm is card breaches and that large card breaches are the most damaging. Strangely, larger firms may be more susceptible to card breaches and therefore managers of large firms may need to expend more energy more resources on data security that small firms. This correlational result may be due to the profit motive of those who wish to obtain such information. That is larger targets may have larger value to steal. Finally, managers should not become complacent after a breach has occurred because subsequent breaches appear to be just as costly, but no more costly, as first time breaches.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. *WEIS (Workshop on the Economics of Information Security) Conference proceedings,* Robinson College, University of Cambridge, England June 26-28.

Binder, J. & Summer, J. (1985). Measuring the effects of regulation with stock price data. *Rand Journal of Economics,* 16(2),167-183.

Brown, S.J. & Warner, J.B. (1980). Measuring security price performance. *Journal of Financial Economics,* 8(3), 205-258.

Brown, S.J. & Warner, J.B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics,* 14(1), 3-31.

Campbell, K., Gordon, L.A., Loeb, M.P., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market. *Journal of Computer Security*, 11(3), 431-448.

Cavusoglu, H. Mishra, B., & Raghunathan, A. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), 69-104.

Garg, A., Curtis, J., & Harper, H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management and Computer Security*, 11(2), 74-83.

Gatzlaff, K. M., & McCullough, K.A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review,* 13(1), 61-83.

Hovav, A. & D'Arcy, J. (2003). The Impact of Denial-Of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6(2), 97-121.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce 12(1), 69-91*

Ponemon Institute, (2015). Cost of data breach study: Impact of business continuity management. IBM 2015.

Privacy Rights Clearing House, (2014). Chronology of Data Breaches. https://www.privacyrights.org/data-breaches (last accessed March 6, 2017)

Spiderlabs, Trustwave Global Security Report, (2015). https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf (last accessed March 6, 2017)